AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions of claims in the application:

Listing of Claims:

1. (Currently Amended) A security analysis tool for an automation system, comprising:

an interface component that generates a description of one or more industrial controllers, wherein the description includes at least one of shop floor access patterns, Intranet access patterns, Internet access patterns, ~~and~~ or wireless access patterns;

an analyzer component that generates one or more security outputs based on the description, the one or more security outputs including at least one output deployed to the one or more industrial controllers that adjusts a security parameter associated with the one or more industrial controllers; and

a validation component that periodically monitors the one or more industrial ~~network~~ controllers following deployment of the one or more security outputs to determine one or more vulnerabilities related thereto ~~and automatically installs one or more security components in response to the one or more vulnerabilities~~.

2. (Currently Amended) The tool of claim 1, at least one of the interface component ~~and~~ or the analyzer component operate on a computer and receive one or more factory inputs that provide the description.

3. (Currently Amended) The tool of claim 2, the factory inputs include at least one of user input, model inputs, schemas, formulas, equations, files, maps, ~~and~~ or codes.

4. (Currently Amended) The tool of claim 2, the factory inputs are processed by the analyzer component to generate the security outputs, the security outputs including at least one of manuals, documents, schemas, executables, codes, files, e-mails, recommendations, topologies, configurations, application procedures, parameters, policies, rules, user procedures, ~~and~~ or user practices that are employed to facilitate security measures in an automation system.

5. (Currently Amended) The tool of claim 1, the interface component includes at least one of a display output having associated display objects and at least one input to facilitate operations with the analyzer component, the interface component is associated with at least one of an engine, an application, an editor tool, a web browser, ~~and~~ or a web service.

6. (Currently Amended) The tool of claim 5, the display objects include at least one of configurable icons, buttons, sliders, input boxes, selection options, menus, ~~and~~ or tabs, the display objects having multiple configurable dimensions, shapes, colors, text, data and sounds to facilitate operations with the analyzer component.

7. (Currently Amended) The tool of claim 5, the at least one input[[s]] includes receiving user commands from at least one of a mouse, keyboard, speech input, web site, remote web service, camera, ~~and~~ or video input to affect operations of the interface component and the analyzer component.

8. (Currently Amended) The tool of claim 1, the description includes a model of one or more industrial automation assets to be protected and associated network pathways to access the one or more industrial automation assets.

9. (Currently Amended) The tool of claim 1, the description includes at least one of risk data ~~and~~ or cost data that is employed by the analyzer component to determine suitable security measures.

10-11. (Cancelled).

12. (Currently Amended) A security analysis method, comprising:

inputting at least one model related to one or more industrial controllers;

~~monitoring access to the industrial controllers to learn at least one access pattern;~~

generating one or more security outputs based on the at least one model; and

automatically installing one or more security components based at least in part on the one or more security outputs[[.]];

monitoring access to the one or more industrial controllers for a predetermined training period to learn at least one access pattern; and

performing at least one automated security event if a detected deviation from the at least one access pattern exceeds a tolerance after the training period.

13. (Currently Amended) The method of claim 12, wherein inputting the at least one model includes inputting ~~the~~ at least one model that is related to at least one of a risk-based model ~~and~~ or a cost-based model.

14. (Currently Amended) The method of claim 12, wherein generating the one or more security outputs includes generating ~~the~~ one or more security outputs that include at least one of recommended security components, codes, parameters, settings, related interconnection topologies, connection configurations, application procedures, security policies, rules, user procedures, ~~and~~ or user practices.

15. (Currently Amended) The method of claim 12, further comprising ~~at least one of~~:

automatically deploying the one or more security outputs to ~~one or more entities~~ the one or more industrial controllers; and

utilizing the one or more security outputs to mitigate at least one of unwanted network access ~~and~~ or network attack.

16. (Currently Amended) A security analysis system in an industrial automation environment, comprising:

means for receiving abstract descriptions of one or more industrial controllers;

means for learning at least one access pattern for accessing the one or more industrial controllers;

means for generating one or more security outputs based on the abstract descriptions;

means for automatically distributing the one or more security outputs to facilitate network security in the industrial automation environment;

means for automatically detecting a deviation from the at least one access pattern that exceeds a threshold; and

means for performing an automated action that alters a current access pattern based at least in part on the detected deviation.

17. (Currently Amended) A security validation system, comprising:

a scanner component [[to]] that automatically interrogates an industrial automation device at periodic intervals for security related data;

a validation component [[to]] that automatically assesses security capabilities of the industrial automation device based upon a comparison of the security related data and one or more predetermined security guidelines;

a security analysis tool that recommends interconnection of one or more industrial automation devices to achieve a specified security goal; and

a component [[to]] that automatically ~~install one or more security components~~ adjusts at least one security parameter in the industrial automation device in response to detected security ~~problems~~ events.

18. (Cancelled).

19. (Currently Amended) The system of claim 17, the validation component performs at least one of a security audit, a vulnerability scan, a revision check, an improper configuration check, file system check, a registry check, a database permissions check, a user privileges check, a password check, ~~and~~ or an account policy check.

20. (Original) The system of claim 17, the security guidelines are automatically determined.

21. (Previously Presented) The system of claim 46, the host-based component performs vulnerability scanning and auditing on devices, the network-based component performs vulnerability scanning and auditing on networks.

22. (Cancelled).

23. (Currently Amended) The system of claim 21, at least one of the host-based component ~~and~~ or the network-based component at least one of ~~includes~~ non-destructively ~~mapping~~ maps a topology of information technology (IT) and industrial automation devices, ~~checking~~ checks revisions and configurations, ~~checking~~ checks user attributes, ~~and~~ or ~~checking~~ checks access control lists.

24. (Cancelled).

25. (Currently Amended) The system of claim 17, further comprising a component that initiates a security action in response to the detected security events, the security action includes at least one of automatically correcting the security ~~problems~~ events, automatically adjusting security parameters, altering network traffic patterns, add security components, removing security components, firing alarms, automatically notifying entities about detected problems and concerns, generating an error or log file, generating a schema, generating data to re-configure or re-route network connections, updating a database, ~~and~~ or updating a remote site.

26. (Currently Amended) An automated security validation method, comprising:

scanning one or more industrial automation devices for potential security violations at periodic intervals, wherein identity information about end devices ~~that relates to~~ having potential for hacker entry is gained;

performing an automated security procedure that adjusts at least one security parameter on the one or more industrial automation devices based at least in part on the potential security violations; and

determining whether the one or more industrial automation devices conforms to one or more ~~industry~~ network security standards following performing the automated security procedure thereon.

27. (Currently Amended) The method of claim 26, further comprising at least one of:

checking for susceptibility to network-based attacks;

searching for open Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ports; ~~and~~ or

scanning for vulnerable network services.

28. (Currently Amended) The method of claim 26, further comprising at least one of:

automatically performing security assessments;

automatically performing security compliance checks; ~~and~~ or

automatically performing security vulnerability scanning.

29. (Currently Amended) The method of claim 26, wherein performing an automated security procedure includes performing ~~the~~ an automated security procedure[[s]] that includes at least one of automatically performing corrective actions, altering network patterns, adding security components, removing security components, adjusting security parameters, ~~and~~ or generating security data to mitigate network security ~~problems~~ events.

30. (Currently Amended) An automated security validation system, comprising:

means for scanning one or more industrial automation devices for potential security violations;

means for initiating a security procedure that adjusts at least one security parameter in the one or more industrial automation devices in response to the potential security violations; ~~and~~

means for performing at least one of security assessments, security compliance checks, ~~and~~ or security vulnerability scanning of the one or more industrial automation devices to mitigate the security violations based at least in part on the initiated security procedure; and

means for determining whether the automated security validation system conforms to one or more ~~industry~~ network security standards based on at least one of the security assessments, the security compliance checks, ~~and~~ or the security vulnerability scanning.

31. (Currently Amended) A security learning system for an industrial automation environment, comprising:

a learning component [[to]] that monitors and learns industrial automation activities during a training period; and

a detection component [[to]] that automatically triggers a security event based upon detected deviations of subsequent industrial automation activities after the training period, wherein the security event includes ~~automatically installing one or more security components~~ adjusting at least one security parameter associated with the industrial automation environment.

32. (Currently Amended) The system of claim 31, the industrial automation activities include[[s]] at least one of a network activity ~~and~~ or a device activity.

33. (Currently Amended) The system of claim 31, the learning component including at least one of a learning model ~~and~~ or a variable

34. (Currently Amended) The system of claim 31, the industrial automation activities include at least one of a number of network requests, a type of network requests, a time of requests, a location of requests, status information, ~~and~~ or counter data.

35. (Currently Amended) The system of claim 31, the detection component employs at least one of a threshold ~~and~~ or a range to determine the deviations.

36. (Currently Amended) The system of claim 35, the at least one of the threshold ~~and~~ or the range are dynamically adjustable.

37. (Currently Amended) The system of claim 33, the learning model includes at least one of mathematical models, statistical models, probabilistic models, functions, algorithms, ~~and~~ neural networks, classifiers, inference models, Hidden Markov Models (HMM), Bayesian models, Support Vector Machines (SVM), vector-based models, ~~and~~ or decision trees.

38. (Currently Amended) The system of claim 31, the security event further includes at least one of automatically performing corrective actions, altering network patterns, adding security components, removing security components, adjusting security parameters, firing an alarm, notifying an entity, generating an e-mail, interacting with a web site, ~~and~~ or generating security data to mitigate network security problems.

39. (Currently Amended) A security learning method, comprising:

monitoring a network of industrial controllers for a predetermined time;

automatically learning at least one data transfer pattern of the network of industrial controllers during the predetermined time; ~~and~~

generating an alarm and altering network activity to adjust a current data transfer pattern ~~where a~~ if the current data transfer pattern is determined to be outside of a predetermined threshold ~~associated with one or more industry standards~~.

40. (Currently Amended) The method of claim 39, further comprising:

employing the at least one data transfer pattern ~~employed~~ as input for a security analysis process[[.]]; and

adjusting at least one security parameter associated with the network of industrial controllers based on the security analysis process and the input.

41. (Currently Amended) A security learning system in an automation environment, comprising:

means for scanning a network;

means for learning access patterns to at least one industrial automation device from the network; and

means for generating a security event ~~where~~ that disables network requests from at least one outside network upon determining that the access patterns are ~~determined to be~~ out of tolerance ~~from~~ with stored access patterns ~~as compared to one or more industry standards~~.

42-44. (Cancelled).

45. (Previously Presented) The tool of claim 1, the analyzer component is adapted for partitioned security specification entry and sign-off from various groups.

46. (Currently Amended) The system of claim 17, the scanner component and the validation component are at least one of a host-based component ~~and~~ or a network-based component.

47. (Currently Amended) The system of claim 21, at least one of the host-based component ~~and~~ or the network-based component at least one of determines susceptibility to common network-based attacks, searches for open Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ports, scans for vulnerable network services, attempts to gain identity information about end devices that relates to hacker entry, or performs vulnerability scanning and auditing on firewalls, routers, security devices, and factory protocols.

48. (New) The system of claim 1, the validation component automatically installs one or more security components in response to the one or more vulnerabilities.

49. (New) The system of claim 1, wherein the analyzer component further performs an automated action that alters access patterns to the one or more industrial controllers upon detecting a deviation from the at least one of shop floor access patterns, Intranet access patterns, Internet access patterns, or wireless access patterns in excess of a threshold.

50. (New) The system of claim 12, wherein the at least one automated security event includes at least disabling network attempts to access the one or more industrial controllers.